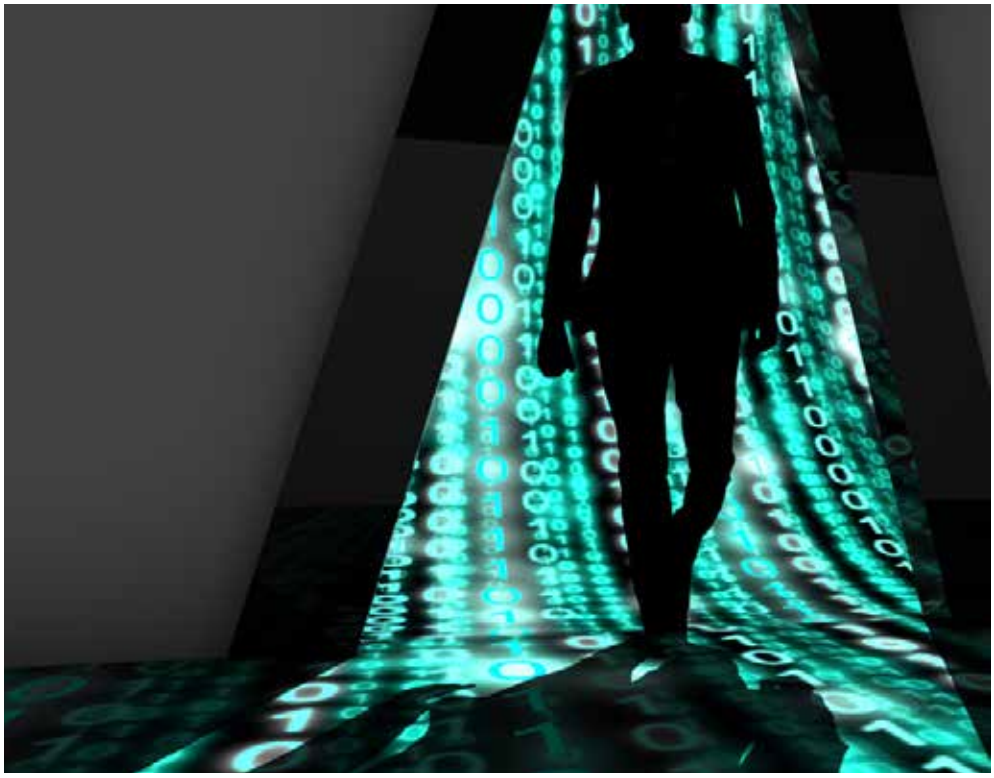
Lacy Rex
Associate Client Executive
513.716.6002
lrex@oswaldccompanies.com

Social Engineering Fraud:

Evaluating for Gaps and Overlaps

By Lacy Rex



Cyber crime is a booming business for criminals. Businesses of all sizes are being targeted for scams that range from tech support scams to phishing attacks and telecommunications fraud. With the ability to outsource services via 'Crime as a Service' (CaaS), it lowers the bar for entry into cyber crime. This offering provides the tools for someone lacking technical knowledge to buy services to carry out cyber crime. CaaS allows the most unsophisticated criminals to utilize harmful technology.

Another challenge for law enforcement is that cyber crime is difficult to track. The FBI estimates that only 15% of fraud is reported by their victims[1]. According to the FBI's Internet Crime Complaint Center report, in 2016 they received 298,728 complaints with reported losses in excess of $1.3 billion. If we factor in the estimated unreported cyber crimes, that number is a little under $9 billion.[2]

Historically, crime policies have been fairly static. Until recently, there has not been a need to evaluate the coverages and endorse the crime policies. The new and emerging trends have changed the landscape for this coverage, such as:

- Social engineering fraud
- Business email compromise/ e-mail account compromise
- CEO Fraud
- Telecommunications fraud
- Computer fraud

The evolving crime and cyber environment has necessitated a need to coordinate coverage between the cyber policy and the crime policy. Traditionally crime is theft of money and cyber is theft of data. As the lines of coverage begin to blur, cyber liability carriers are adding grants of coverage for cyber crime and crime markets are adding cyber coverage.

It is important to coordinate the "Other Insurance" provision in both policies if there is duplicate coverage. This should assist in the event of a claim and determine which is primary and which is excess. Every organization should work with their insurance broker to evaluate potential gaps in coverage and overlaps as well.

www.oswaldccompanies.com

oswald

[1]The United States Attorney's Office, Western District of Washington; Financial Crime Fraud Victims. http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud
[2]https://krebsonsecurity.com/2017/06/fbi-extortion-ceo-fraud-among-top-online-fraud-complaints-in-2016
https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf
http://www.databreachtoday.co.uk/interviews/crome-as-a-service-top-cyber-threat-for-2017-i-3406